1. Introduction

1.1. Cryptographic Smart Card

- TIMECOS
- Employ 32-bit microprocessor security chip design capable of making USB communications.
- FIPS140-2(US Federal Information Processing Standards) compatible.
- Highly secured, supports 1024-bit and 2048-bit RSA asymmetrical encryption algorithm, and generates RSA key pairs inside card.
- Supports with the ability to produce 1024-bit and 2048-bit RSA signature, verify, encryption, decryption.
- Provides multiple Security Algorithms: DES, 3DES, MAC, SHA-1, SHA-256 , AES optional.
- Supports 64KB EEPROM
- Complies to USB1.1 standard and USB 2.0 full speed

1.2. Software/Middleware

- Support X.509V3 certificate format
- Supports ISO7816 part4 file structures: transparent, linear fixed, linear variable, cyclic.
- Supports ISO7816 part8/9 security related interindustry commands and security attributes.
- Supports PC/SC protocol or USB Mass Storage.
- Supports Microsoft CAPI2.0, PKCS#11 v2.11, PKCS#1,7,8,10 and12, PKCS#15

- ✧ Supports Windows98/2000/XP/2003/Vista/Win7 environment.
- ✧ Supports Internet Explorer 5 or above, Mozilla Firefox and Netscape.

1.3. Specifications

Supported operating systems	Windows 2000/XP/Vista/2003/Windows 7
Supported browsers	Internet Explorer 5.0+; Firefox 3.0+ ; Netscape
API & standards support	PKCS#11 v2.01, Microsoft CAPI 2.0, PC/SC, X.509 v3 certificate SSL v3,
Memory Size	64K
On board security algorithms	RSA 1024-bit and 2048-bit, DES, 3DES (Triple DES), MAC , AES SHA-1, SHA-256
Security certifications	smart card chip: FIPS 140-2
ISO specification support	Support for ISO 7816-1 to 4 ,8/9 specifications
Operating temperature	0° C to 70° C (32° F to 158° F)
Storage temperature	-40° C to 85° C (-40° F to 185° F)
Humidity rating	0-100% without condensation
Connector	USB type A; supports USB 1.1 and 2.0 (full speed and high speed)
Memory data retention	At least 10 years
Memory cell rewrites	At least 500,000
Weight and Size	Approx. 8g , 78mm*23mm*9mm

2. WatchSAFE ND 3.4 Installation

AutoRun supported ND (No Driver) USBKey integrated installation program inside itself. In OS (Operating System) which allows CD automatic running, the installation of management tool will automatically run when USBKey plugged in.

For other ND USBKey, a management tool installation from CD is needed. In this chapter, the installation and uninstall of WatchSAFE ND 3.4 will be illustrated.

2.1 Install WatchSAFE ND 3.4

At the first time of plugging in ND USBKey, the auto-run supported product will automatically install certificate management tool in the OS which allows CD automatic running. For using other USBKeys, it is necessary to install the tool from CD at first.

Installation process:
At the first time of inserting USBKey, an installation window like figure 2.1.1 will pop out. In a few seconds, you will find a window displaying successfully installed.

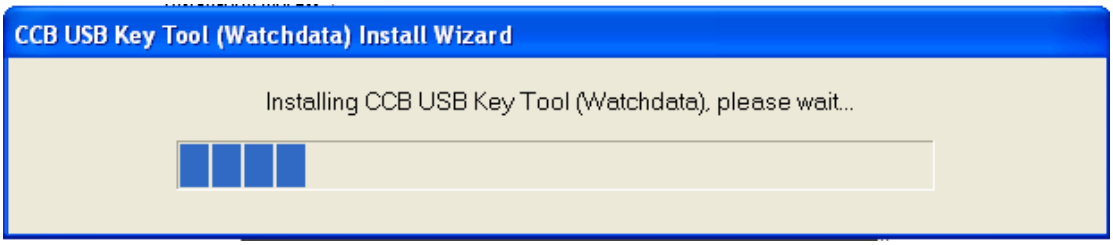

Figure 2.1.1 China Construction Bank's USBkey auto-installation

2.2 Uninstall WatchSAFE ND 3.4

There're two methods for uninstalling the tool:

1. In 'Control Panel', using 'Add/Remove Programs' to delete 'WD Ukey User Tool v3.4'.
2. Using the 'Uninstall' option in the subcategory of 'Start' -> 'All Programs' -> 'WD UKey Tool v3.4'.

Step 1: upon select 'uninstall', a window like figure 2.2.1 appears.

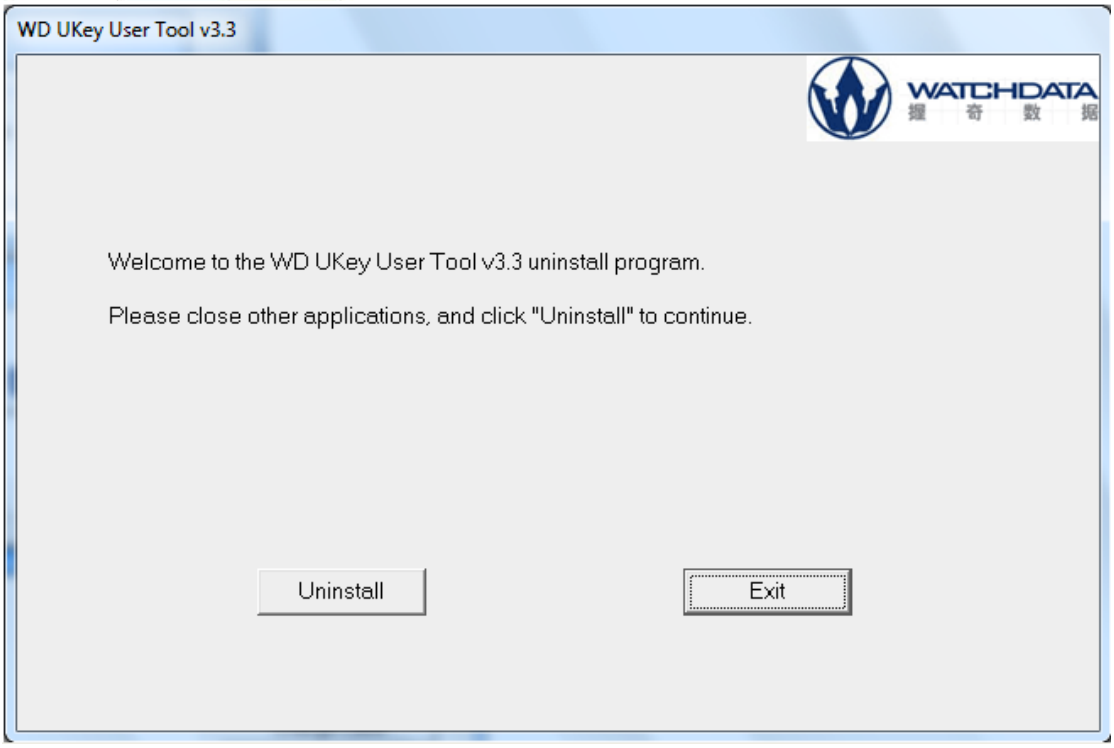

Figure 2.2.1 First page of USBkey uninstall

Step2: click the 'Uninstall' button, then a new window like figure 2.2.2 will come out. Click the 'OK' button to finish uninstall operation.

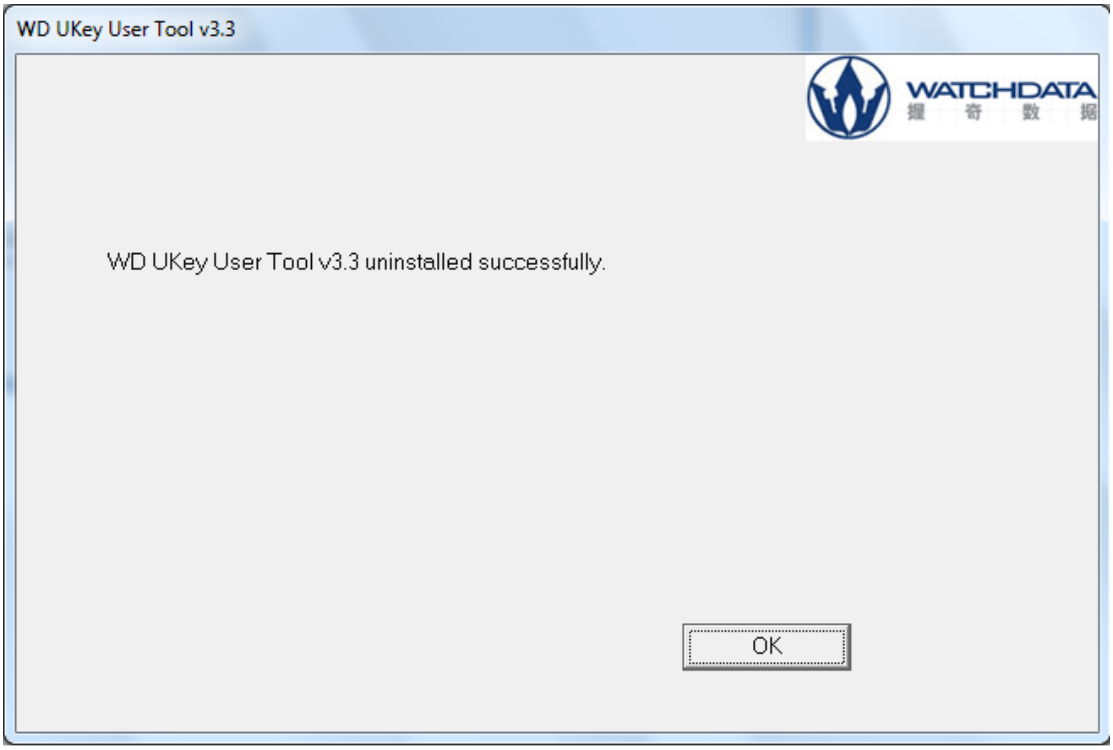

Figure 2.2.1 Complete uninstalled

3.WatchSAFE ND 3.4 user's tool

WatchSAFE ND 3.4 user's tool is mainly used to achieve the following functions:

- Verify password
- Change password
- Check system
- Change label
- Show certificate
- Register certificate
- Revoke certificate

In this chapter, the operations to implement the above functions will be illustrated.

3.1 Start WatchSAFE ND 3.4 user's tool

WatchSAFE ND 3.4 user's tool can be started by click 'WD UKey User Tool v3.4' in the route of 'Start' -> 'All Programs' -> 'WD UKey Tool v3.4'. It is also available by double-click the shortcut on desktop.

When WatchSAFE ND 3.4 user's tool is running, the label of the tool will be displayed at the right bottom corner as figure 3.2.1.

Figure 3.2.1 running label of WatchSAFE ND 3.4 user's tool

3.2 Exit WatchSAFE ND 3.4 user's tool

Click the 'close' button at upper right corner to exit WatchSAFE ND 3.4 User Interface.

3.3 The use of WatchSAFE ND 3.4 user's tool

3.4.1 Multi-Key operation

When more than one USBKeys plugged in, you can select a device as you need. It is illustrated in figure 3.1.1 that there are two available USBKeys: *WatchSAFE_UDKaaa* and *WatchSAFE_UDK*.

3.4.2 Verify Password

This function is designed for provide a better PIN management platform.

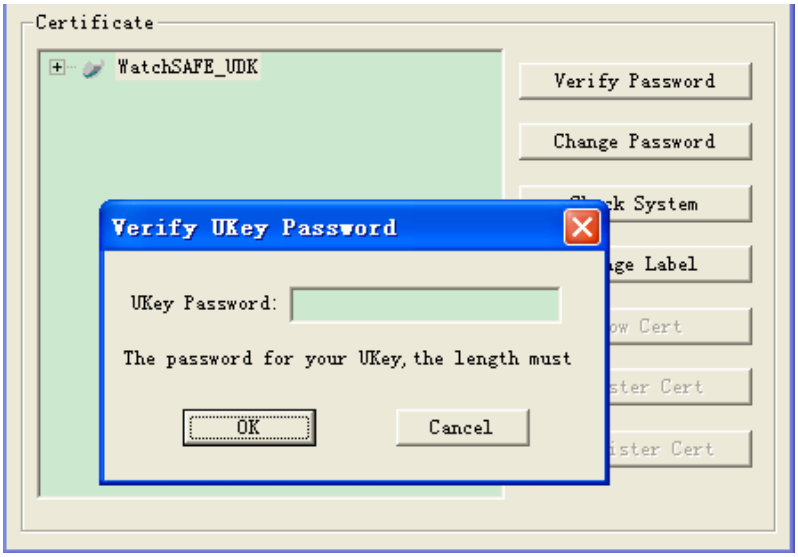

Figure 3.4.2.1 the UI of change password

3.4.3 Change Password

The function of change password provides a better security for the key's holder and prevents embezzlement.

Figure 3.4.3.1 the UI of change password

For example, the PIN of USBKey is initially set as '111111'. But, for security purpose, it should be changed into a secret PIN which is only known by the user.

If wrong PIN is entered, a prompt will appear and display the number of available PIN retry times.

If PIN is retried more than the maximum, the USBKey will be automatically locked. Then, the USBKey can only be unlocked by the issuer.

3.4.4 Check System

The function of system checking provides users with clear information about the system and the USBKey status.

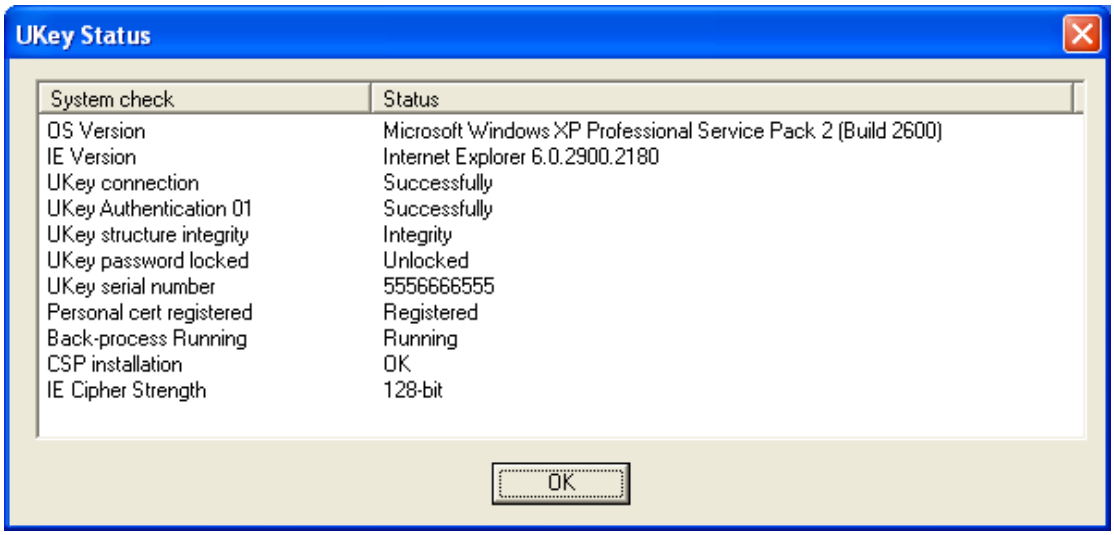

Figure 3.4.4.1 system checking

3.4.5 Change Label

The function of change label is designed for help users identify USBKey.

Figure 3.4.5.1 the UI of change label

3.4.6 Show Certificate

After an USBKey is selected, WatchSAFE ND 3.4 user's tool will list all the available certificates. Choose a certificate and press 'Show Cert' button, a new window like figure 3.4.6.1 will display the certificate's details which include issuer name, valid date and so on.

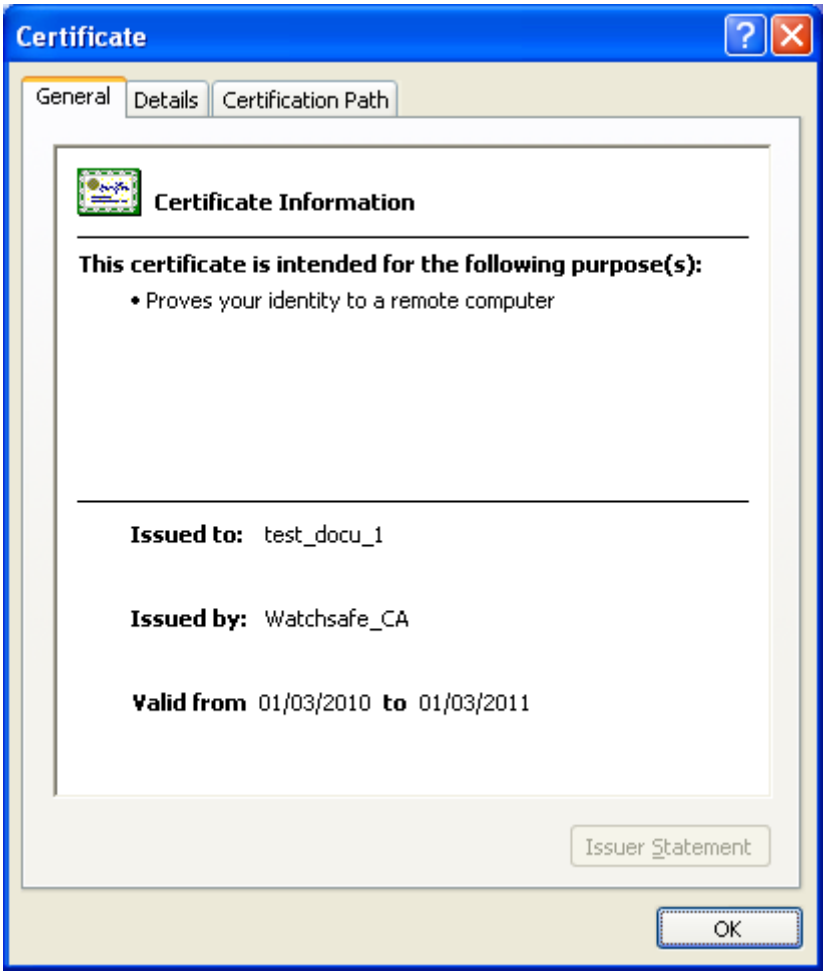

Figure 3.4.6.1 certificate information

4. Benefits

- ✧ **Simple:** Plug and play simplicity for users, with no end-point software installation
- ✧ **Strong Security:** Certificate-based authentication with onboard smartcard
- ✧ **Interactive:** LED light displays power and communication status
- ✧ **Conveniently:** small and portable, easy to use.
- ✧ **Application Rich:** Ideal for expanding online services and offering simple and secure access to partners, customers and mobile workers from any location

5. Typical Applications

- ✧ Online Banking
- ✧ E-government
- ✧ Identification authentication on network
- ✧ Secure e-commerce and secure remote access
- ✧ Public Key Infrastructure based Application
- ✧ PKCS#11 & CSP-compliant software applications
- ✧ Customized applications

6. Compliance Statement

15.19(a)(3)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

15.21

Caution: The user is cautioned that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

15.105(b)

For a Class B digital device or peripheral, the instructions furnished the user shall include the following or similar statement, placed in a prominent location in the text of the manual:

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.